EUROPEAN FINANCIAL CONGRESS

Instytut Badań
nad Gospodarką Rynkową
Do Studzienki Str. 63
80-227 Gdańsk, Poland

tel. +48 58 524 49 01
fax. +48 58 524 49 09

efc@ibngr.pl
www.efcongress.com

Position of the European Financial Congress[1] in relation to the European Banking Authority's discussion paper on the Approach to Financial Technology (FinTech)[2]

Methodology for preparing the answers

The answers were prepared in the following stages:

Stage 1

A group of experts from the Polish financial sector were invited to participate in the survey. They received selected extracts of the EBA's discussion paper and the consultation questions in Polish. The experts were guaranteed anonymity.

Stage 2

The survey project coordinators from the European Financial Congress prepared a draft synthesis of opinions submitted by the experts. Responses were obtained from experts representing:

- banks,
- fintech companies,
- insurance companies,
- regulatory institutions,
- consulting and law firms,
- the academia.

The draft synthesis was sent to the experts participating in the survey with the request to mark the passages that should be modified in the final position and to propose modifications and additions as well as marking the passages they did not agree with.

Stage 3

On the basis of the responses received, the final version of the European Financial Congress' answers was prepared.

[1] European Financial Congress (EFC – www.efcongress.com). The purpose of the EFC is to promote debate on how to ensure the financial security and sustainable development of the European Union and Poland.
[2] http://www.eba.europa.eu/documents/10180/1919160/EBA+Discussion+Paper+on+Fintech+%28EBA-DP-2017-02%29.pdf

Answers of the European Financial Congress to the consultation questions

1. Are the issues identified by the EBA and the way forward proposed in section 4.1 relevant and complete? If not, please explain why.

Most of the entries accurately reflect the situation. A sound observation was that there is no regulation or supervision for a wide range of institutions, including those defined as fintechs and operating in the financial field.

Supervision and regulations should cover individual entities depending on the actions they actually carry out, their nature and scale, and not their formal method of functioning on the market. Fintech status should not be a reason for better treatment. On competitive markets with a high level of innovation, such as Poland, there are no reasons why any chosen entities should receive preferential treatment because of their character.

Sandbox type solutions and facilitations, if any appear, should apply to every entity, including banks, and not just fintechs, as long as sandbox tested solutions meet uniform criteria (values, volumes, etc.). Of course, in practice this would affect fintech start-ups.

Of key importance for supervision should be to maintain system security and client security, regardless of the type of institution providing the financial or banking services for the clients.

As far as innovativeness is concerned, it may prove useful to retain freedom at a national level, with knowledge then being exchanged and best practices introduced at a European level.

2. Are the issues identified by the EBA and the way forward proposed in subsection 4.2.1 relevant and complete? If not, please explain why.

Yes, these are apt and properly indicate the direction.

One element which seems worth mentioning, and which complements the further steps proposed by the EBA, is a strengthening of collaboration and knowledge sharing among supervisory bodies in member states.

In the field of cybersecurity, it is worth pointing out that security is as strong as its weakest link. Allowing less-regulated entities to enter banking systems on a large scale, as mentioned in PSD2 (PIS and AIS services), carries with it a significant systemic risk for the banking sector, since without contracts a bank will have no influence on the management of data in the hands of third party providers (TPP), and gaps in the fintech systems (less regulated or outside the regulations) could in practice affect the outflow of bank customers' money and data. This shows how proper it is to subject TPPs to broad supervision. The risk indicated here may be visible in the long term. The outflow of bank data from fintechs may have a negative effect not only on fintech entities, but also on the banking sector and it could weaken trust in the banking sector.

3. What opportunities and threats arising from FinTech do you foresee for credit institutions?

Selected opportunities:

- increased innovativeness of financial institutions' business models,
- further digitization of the business model,
- greater flexibility,
- wider analysis of data and information, opportunity to build better scoring and risk assessment models,
- further automation of customer service processes, including limiting costs and human error,
- reduction of the operating costs of financial institutions,
- faster provision of services (faster decision making, e.g. regarding loans,
- new business models.

Threats:

- if financial scoring is approached superficially in the fintech model (quicker financial decisions based on data from external sources) it will be less reliable,
- breach of the security, confidentiality and integrity of data,
- uneven competition: fintech firms are unregulated or less regulated entities offering the same products as highly regulated banks; as a result fintech firms may gain competitive advantage over banks in the short-run but in the long-run fintech firms will generate much higher risk,
- loosening of banks' relations with their customers and making it difficult to offer cross sell
  and package services, thus placing banks in a much worse competitive situation compared to the fintech institutions being promoted,
- supervision becoming more difficult,
- risks arising from less rigorous security in unregulated entities,
- an increase in cyberthreats (e.g. new models for taking over bank accounts),
- the appearance of new risks connected with new business models.

4. Are the issues identified by the EBA and the way forward proposed in subsection 4.2.2 relevant and complete? If not, please explain why.

It is of critical importance in financial services to maintain the security of the system and of customers. It is vital to strike a balance between developing innovative forms of payment and maintaining the optimum level of security and trust with regard to electronic payment methods. Banks should be able to set their own policies in this area.

With regard to DLT and Blockchain, the EBA should collect analyses by central banks and the financial sector, and use these as a basis for its own proposed analyses and the recommendations arising from these.

Because of the variation among EU markets, it may not be possible to produce unified conclusions, and this could create risk for certain markets (particularly those with more effective supervision).

5. What opportunities and threats arising from FinTech do you foresee for payment institutions and electronic money institutions?

Similar to pt. 3, in particular:

Opportunities:

- more efficient cross-border payments,
- better access to services and faster provision of services,
- further development of cashless payments,
- lower costs for cross-border transactions,
- robo-advisory solutions,
- new methods for identifying and authenticating users, in particular biometrically, including for payment purposes.

Threats:

- increased risk of fraudulent transactions,
- AML risk (particularly in cross-border and P2P payments),
- breach of the security, confidentiality and integrity of data,
- breach of the principles of fair competition, by promoting or limiting the requirements for entities depending on their status (fintechs).

6. Are the issues identified by the EBA and the way forward proposed in subsection 4.3.1 relevant and complete? If not, please explain why.

The position does not require additional comment. The need to share knowledge may have to be stressed.

7. What are your views on the impact that the use of technology-enabled financial innovation and/or the growth in the number of FinTech providers and the volume of their business may have on the business model of incumbent credit institutions?

- further digitization and automation,
- cost reduction,

- falling profit margins (systemic risk for regulated entities due to the high "regulatory" costs),
- improvement of service quality,
- limiting the availability of new services for digitally excluded people,
- greater systemic risk,
- lower customer security levels as a result of increasingly common use of unregulated new entities (which in practice often offer a lower level of security).

8. Are the issues identified by the EBA and the way forward proposed in subsection 4.3.2 relevant and complete? If not, please explain why.

These questions have not yet been defined, so they are difficult to assess.

Interviews should be carried out with a wider range of entities, in particular regulators, banks, payment institutions and so-called fintechs. CERT entities are also worth considering in the discussion.

9. What are your views on the impact that the use of technology-enabled financial innovation and/or the growth in the number of FinTech providers and the volume of their business may have on the business models of incumbent payment or electronic money institutions?

- financial innovations based on new technologies are causing a change in the approach and evolution of business models,
- acceleration of the evolution of banks,
- greater systemic risk as a derivative of faster changes,
- difficulties for the regulators to keep up with changes,
- excessive focus on convenience at the cost of security, which, particularly in the long term, may prove dangerous (digital security will not be sufficient).

10. Are the issues identified by the EBA and the way forward proposed in subsection 4.4.1 relevant and complete? If not, please explain why.

Consumer protection is a key factor, regardless of what entity is providing financial or payment services, or of which country a supplier is from and also, regardless of this, which entities collaborate with one another to provide a given service (including the legal form of their collaboration). Cooperation among regulators will be of great importance.

11. Are the issues identified by the EBA and the way forward proposed in subsection 4.4.2 relevant and complete? If not, please explain why.

The EBA has rightly noted the particular problem of consumer rights protection in the situation where cross-border services are being provided, especially in the context of limited harmonization of legislation in member states, and the related problem of regulatory arbitration and practices used by entrepreneurs, involving contractual exclusion of the jurisdiction of courts of the state where the consumer is resident, in favour of the courts in the country where the entrepreneur is headquartered.

Cooperation among regulators will be of great importance.

12. Have you experienced any regulatory obstacles from a consumer protection perspective that might prevent FinTech firms from providing or enabling the provision of financial services cross-border?

Regulatory obstacles in the case of cross-border financial services, with the potential to make them impossible, seem to result mainly from the lack of clarity about what legislation, from which of the countries where the services are provided, will be applied to consumer protection.

The lack of consistent regulations in this area is a problem not only for fintech companies, but for all institutions operating across borders (including credit institutions, payment institutions and electronic money institutions), and any simplifications should concentrate on easing cross-border activity in itself, rather than on making fintechs' business easier.

The GDPR regulations coming into force may limit the risk connected with personal data protection.

In practice, however, when looking at the development of fintechs, regulatory obstacles connected with consumer protection do not seem to have excessively hindered or prevented the provision of cross-border financial services.

13. Do you consider that further action is required on the part of the EBA to ensure that EU financial services legislation within the EBA's scope of action is implemented consistently across the EU?

Yes. It is necessary here to take the specific nature of local markets into consideration, to enable innovativeness at a European and also a local level, and to consider elements which are local and not covered by plans for standardization (e.g. local deposit guarantee systems).

It is also worth adding that banks in particular are already over-regulated, and caution should be applied with regard to imposing new obligations, so that these do not become unjustified duties paralleling those which already exist. This problem does not, of course, affect entities which are currently unregulated.

14. Are the issues identified by the EBA and the way forward proposed in subsection 4.4.3 relevant and complete? If not, please explain why.

At the current stage of fintech market development, the issues are relevant. Doubts arise from a lack of direct reference to bank/fintech contact if a customer submits a complaint to a bank which is obliged to recognize the claim and seek financing from third parties.

It is worth having this area subject to supervisory regulation in order to avoid regular crediting of this type of claim by account providers, or the necessity to bear unjustified costs to recover such amounts due.

15. Are the issues identified by the EBA and the way forward proposed in subsection 4.4.4 relevant and complete? If not, please explain why.

The matters are well defined. The principles for transparent communication of information to customers should be uniform for all providers of banking/payment services, regardless of the form of their business.

16. Are there any specific disclosure or transparency of information requirements in your national legislation that you consider to be an obstacle to digitalisation and/or that you believe may prevent FinTech firms from entering the market?

There are no regulations to discriminate against fintechs for being fintechs.

There are, however, many regulations imposing various obligations, which constitute natural barriers. Nevertheless, one may not expect that fintech firms should be exempt from those obligations only because they are fintechs.

It should be borne in mind, though, that the current players, and particularly banks, must satisfy much more stringent legal requirements which, while being of fundamental importance for their security, put banks in a worse competitive position compared to the new entities. National payment institutions already have to meet a range of requirements, although significantly lower than banks.

17. Are the issues identified by the EBA and the way forward proposed in subsection 4.4.5 relevant and complete? If not, please explain why.

The matters were described appropriately, but it should still be noted that while customers' knowledge about local national law may be described and presented (which still is not easy to do in an accessible way), when it comes to signing agreements remotely and based on foreign law and contracts drawn up in another language their knowledge may not be sufficient.

Educating and increasing the knowledge of consumers is undoubtedly a necessary condition for any market to function properly. It is important, however, to be aware that the market is developing at an entirely unprecedented rate. For this reason, it is necessary to implement the best consumer education tools from the point of view of

the latest available knowledge. Nonetheless, even the best education may turn out to be inadequate.

It is also important that the education does not exclusively cover the financial sphere, but also deals with security, particularly cybersecurity.

18. Would you see the merit in having specific financial literacy programmes targeting consumers to enhance trust in digital services?

Undoubtedly so, this is a necessary condition for the further development of digital services. All educational activity can be seen as desirable.

It is also important that the education does not exclusively cover the financial sphere, but also deals with security, particularly cybersecurity.

The creation of new services should involve not only education concerning the benefits of the new services (which in practice means marketing and promotion), but also honest education about the risks and ways of countering them, for example keeping verification data confidential so that it is indeed a security measure known only to the user and the only entity which can check it is the one which issued it.

Also important is the appropriate training for financial sector employees who interact with customers, so that they themselves are aware of the safeguards used in electronic channels, and can explain them to customers.

For example, the use of API as a new method of accessing customer data provides cybercriminals with an opportunity to exploit new attack vectors, both against infrastructure and with the use of social engineering. The acquisition of data from banks could result in the theft of identities as well as money. Due to the importance of the data which can be acquired, it is a challenge to properly educate customers in order to prevent potential abuses of electronic access channels.

19. Are the issues identified by the EBA and the way forward proposed in subsection 4.4.6 relevant and complete? If not, please explain why.

Although the problems are correctly indicated as a general area, it should be noted that the benefits of such methods as big data and AI seem to outweigh any negative effects they may have.

It is not big data or AI which is the problem, just the use of specific types of data. In itself, the process of collecting and analysing data brings many advantages and, contrary to the idea suggested, does not necessarily lead to exclusion, but can effectively enable wider access to services, as it allows products to be offered to some users who have not previously been offered services by banks. Enabling banks to use the methods which fintechs are already using can even out the chances on the dynamically growing market.

A few supplementary ideas can be postulated, such as the question of using AI for virtual advisers such as chatbots in banking services (voice and text chatbots, including

those based on communicators and social media), and not just robo-advisors in the sense of automatic financial advisers (automation in financial advice/advisory).

The material also contains no indication of the risk connected with concentrating such extensive amounts of data on the population of the EU in the hands of a few institutions from outside the EU, such as Facebook, Google, Amazon and Apple.

20. Are the issues identified by the EBA and the way forward proposed in section 4.5 relevant and complete? If not, please explain why.

There is a risk of unfair competition from particularly unregulated entities. Specifically, not all fintechs are subject to PSD 2. It is worth analysing the dependencies and considering the creation of a centralized way of monitoring unfair competitive practices.

The issues described in section 4.5 are of particular importance due to the current and potential scale of fintechs' operations and the possibility for them to influence not only the European, but also the global financial market. The competitive advantage of fintechs often lies in the ease and speed of service obtained at the cost of greater risk, which is a result of supervision being limited or absent.

While observing the market is a first step, it is certainly not enough. Further steps must involve specifying the actions planned in this field.

21. Do you agree with the issues identified by the EBA and the way forward proposed in section 4.6? Are there any other issues you think the EBA should consider?

The issues and comments shown in section 4.6 are presented comprehensively and consistently.

It is worth considering an exchange of knowledge with equivalent institutions outside Europe, and broader sharing of knowledge between supervisors and market participants in order to perfect methods in the field of AML/CFT.

It is rightly noted that all entities should be uniformly subject to the regulations.

22. What do you think are the biggest money laundering and terrorist financing risks associated with FinTech firms? Please explain why.

- speed of money transfers, wide availability of instant payments,
- lack of a wider context to the transaction which would enable identification of the connections between different products and customers – not all actual flows and relationships are visible in classic fintech,
- lack of resources and education in fintech – they are often start-ups where risk awareness comes at a later stage of development,
- banks and other financial institutions function on a strictly regulated market, they are trusted institutions, whereas fintechs are entities whose range of

activities is unregulated, problems experienced by fintechs may also have negative effects on the banking market,

- risk connected with money laundering is an investment matter (acquiring shares in fintechs, risk of investment bubbles) as well as an operational one - uncontrolled financial flows can more easily come from illegal sources,
- fintech services can be used by criminal organizations operating in the field of money laundering or terrorism, who can afford modern IT solutions which can help them legitimize their criminal activities, including those based on the banking infrastructure - fintechs do not have sufficient obligations with regard to information as is the case for banks,
- automation and the speed of the onboarding process used by most fintechs is innately connected with greater imprecision of the process of countering money laundering, which increases this risk,
- the ease with which parties to a transaction can be made anonymous is conducive to criminal activity.

23. Are there any obstacles present in your national AML/CFT legislation which would prevent

a) FinTech firms from entering the market

There are no regulations to discriminate against fintechs for being fintechs.

It is worth pointing out that regulations concerning prevention of money laundering and financing terrorism should first and foremost apply to all entities which conduct monitored transactions - banks, fintechs and all other entities. Every company providing financial products should counter money laundering and financing of terrorism.

b) FinTech solutions to be used by obliged entities in their customer due diligence process? Please explain.

No such limitations can be seen. There are also no precise regulations on the use of biometric identification, for example, by entities which are obliged to. Certain technical solutions applied in the DD process may well be desirable (and already on offer), but a lack of regulation in this field may discourage their wider implementation due to fears about accusations which may arise with regard to the principles and circumstances of their use.

Innovation should only be used by the obliged entities in the due diligence process when it has a positive effect on their efficiency and no negative effect on the stability of the whole system.

24. Other comments

Everybody knows the opportunities brought by fintechs and the new solutions. The fact that the EBA also looked at the risks involved is highly valuable. Such an approach can potentially level out the competitive position of traditional players (mainly banks) and the new entities.

It is also worth mentioning that after PSD2 and RTS (SCA) come into effect, banks will bear full responsibility for payments ordered by third parties, so it is very important to monitor the risk as a whole and per entity. As third parties will receive the possibility of easy access to data about customers' payment accounts and the ability to order payments, they should attach a great deal of importance to customer data protection. The benefits of the EBA initiative can be seen here too.

Finally, the following general elements should be mentioned:

- It is vital to educate all parties – supervisors, regulators, service providers (both banks and fintechs), and customers, so that they can act as safely as possible.
- It is vital that supervisory bodies share their knowledge among themselves and cooperate with the market.
- The pursuit of convenience should not trump the importance of security, which is paramount in the financial sector and is the core reason for the existence of supervisory authorities.
- The level of supervision and regulation should be adequate to the operations and their scale, as well as to the associated systemic and client-related risks, rather than to business status only.